

**AFFIDAVIT IN SUPPORT OF AN APPLICATION**  
**UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE**

I, Jeffrey Stephenson, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

This affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search of a residence, 20 Lewis Street, Springfield, Vermont (hereafter, “the PREMISES”), along with the seizure of all electronic devices found at the PREMISES, further described in Attachment A, and the extraction from those devices of electronically stored information described in Attachment B. As described more fully below, 20 Lewis Street, Springfield, Vermont, is the primary residence of Bradley LEFEBVRE, among others. It is best described as a white two-story wood-sided house located on the west side of Lewis Street, near the intersection of Pine Street. Its paved driveway is on the right side of the residence; there is a small garage near the rear of the residence.

1. I am a Task Force Officer with the Federal Bureau of Investigation (“FBI”) and have been since October 1, 2017. I am assigned to the FBI’s Albany, New York Field Division, Vermont Resident Agency. In such capacity, I am a “federal law enforcement officer” as defined in Federal Rules of Criminal Procedure 41(a)(2)(C), and am authorized to investigate violations of United States Code under Titles 18 and 21, to include applying for search warrants before the United States District Court. I am employed by the Vermont State Police

(“VSP”) as a Detective Trooper and am a certified law enforcement officer in the State of Vermont, having been certified by the Vermont Criminal Justice Training Council for over 14 years. During my career, I have received extensive training related to criminal investigations. I have authored numerous search warrants and participated in hundreds of criminal investigations, many involving the analysis of phone records, digital media, and other electronic communications. Through my training and experience, I am familiar with electronic sources of information related to electronic devices and cellular telephone service providers.

2. The facts in this affidavit come from my observations, training and experience, along with information provided to me by officers with the Springfield (Vermont) Police Department, my review of reports, and documents, and information obtained from witnesses. This affidavit is submitted to show probable cause for a search warrant and does not set forth all my knowledge on this matter.

3. Based on the facts as set forth in this affidavit, there is probable cause to believe that the property described in Attachment A contains information described in Attachment B, as evidence of violations of 18 U.S.C. § 2261A, Stalking.

#### **PROBABLE CAUSE**

4. In or about May 2020 the FBI and VSP began investigating harassment and threats of physical and sexual violence communicated mostly via text message and directed towards John Roger Cawvey Sr. (“Cawvey Sr.”), John Roger Cawvey Jr. (“Cawvey Jr.”), and

Matthew Alldredge (“Alldredge”) who all reside in Springfield, Vermont. My investigation has also identified other victims of similar harassment.

5. On or about May 11, 2020, I interviewed Cawvey Sr. by telephone and learned the following information:

- a. Since about mid-March 2020, John Roger Cawvey Jr. (Cawvey Sr.’s son), had been receiving text messages on both his personal and work cellular phones from an unknown person(s) which were threatening and harassing in nature. Some of the messages were sexually explicit and identified personal information about his family, including his spouse’s employer, his children’s names, and his private residence. The text messages were being sent from multiple phone numbers, but all appeared to be from the same unknown person(s). Some messages included photographs of naked men in states of sexual arousal.
- b. In or about May 2020, Cawvey Sr. began receiving similar messages on his personal cellular phone. These messages referenced Cawvey Jr, his daughter-in-law (Cawvey Jr.’s wife), and his two minor grandchildren (Cawvey Jr.’s children). Cawvey Sr. believed it was the same unknown person(s) sending the messages.
- c. Cawvey Sr, Cawvey Jr, and Matthew Alldredge co-own a business called Retro Automotive Products (“RAP”). The business is located within a large

commercial warehouse, shared by other businesses, at 247J Sullivan Street, Claremont, New Hampshire.

- d. Alldredge has also received similar messages on his cellular phone.
- e. Among the text messages sent to Cawvey Sr, there were at least three instances where it appeared the person(s) responsible was able to monitor what Cawvey Sr. was doing in real time: 1) Cawvey Sr. received messages revealing the sender was aware that Cawvey Sr. had just used the business' bathroom, noting details of his use which only someone who was present or was monitoring the situation could know, 2) after receiving many of these messages, Cawvey Sr. and Cawvey Jr. were inspecting a neighboring business within the warehouse to determine if cameras or some sort of electronic monitoring were present. During this time, Cawvey Sr. received messages indicating the sender would call the police because he was trespassing into someone else's workspace, and 3) when an officer with the Claremont Police Department was present at RAP to investigate these threats, Cawvey Sr. received a text message identifying the specific information about the police officer's physical appearance.
- f. Cawvey Jr. and Cawvey Sr. both received text messages indicating RAP would have problems with the business Internet. When Cawvey Jr. arrived to work that day, he found the Internet was not working. A Comcast technician responded and determined someone had physically disconnected, then

incorrectly re-connected, Internet cables to the business Internet router. The Comcast technician reported it appeared someone intentionally did this to cause Internet outages. Cawvey Jr. and Cawvey Sr. later received text messages from this unknown person(s) taking responsibility for causing the Internet outage. On another occasion, physical damage was found to a cable port on the Internet router. It appeared someone had placed a screwdriver, or similar object, within the port and damaged it.

- g. The Internet router was located within the office area of the business. Although the area was secured from the general public during non-business hours, Cawvey Sr. reported it would be possible to gain access to the area without causing physical damage to the locked doors.
- h. Cawvey Jr. has received text messages discussing his private residence, specifically that his pool cover was falling into the pool, specifics about vehicles parked in his driveway, visitors to his home, and a road rage incident involving his spouse. The person sending the messages claimed to have installed, and later removed, a trail camera capturing images of people/vehicles coming and going from Cawvey Jr.'s driveway. The person(s) sending these messages correctly identified that Cawvey Sr. was the only visitor to Cawvey Jr.'s residence over the course of approximately one week.
- i. On or about May 5, 2020, Cawvey Sr. received text messages from the unknown person(s) threatening to murder his granddaughters and drown them

in the pool. Cawvey Jr. has also received text messages threatening to rape Cawvey Jr's spouse and minor children.

- j. Cawvey Jr. reported he and his family were in constant fear for their safety. They were not allowing the children to go outdoors of the residence unsupervised.

6. On or about May 19, 2020, I interviewed Cawvey Jr. in person and learned the following information:

- a. Cawvey Jr. lives in Springfield, Vermont with his spouse and two minor children. He is a part owner of RAP, a business that resells used Porsche parts worldwide, located in Claremont, New Hampshire. Matthew Alldredge is the primary owner of the business but there are three other co-owners: Cawvey Jr, Cawvey Sr, and one of Alldredge's adult daughters. Alldredge, Cawvey Jr. and one other employee, Bradley LEFEBVRE, are the only people who work at the business on a daily basis.
- b. About two years ago, Cawvey Jr. attended a Christmas party for a former employer. During the party, Cawvey Jr. became intoxicated and was dancing. The following day, he began receiving text messages from an unknown person. The text messages questioned why he had been drinking so much. He never learned the identity of the person who sent the text messages, but they eventually stopped. Cawvey Jr. did not keep a record of the phone number(s) used to text him or the exact dates he received them.

- c. Since on or about March 16, 2020, Cawvey Jr. has been receiving text messages on his personal and work cellular phones from various phone numbers. The messages were threatening and harassing in nature. Many of the messages included homosexual content, images of nude men, and images of men engaging in sexual activity. The messages threatened Cawvey Jr. and his family with sexual assault, unlawful restraint, and physical assaults. Cawvey Jr. did not know the identity of the person(s) sending the messages. He replied to some of the messages to get the sender(s) to stop or identify the person(s) responsible.
- d. Cawvey Jr. received these text messages almost daily, often multiple times per day. They began to escalate into more specific sexual discussion and threats of sexual assault and physical violence directed towards Cawvey Jr.'s spouse and children. The sender began to refer to Cawvey Jr.'s spouse by name and began describing information about his minor children such that one child had a birth defect. The unknown person(s) also sent text messages indicating: 1) the cover on Cawvey Jr.'s pool was falling into the water, 2) claimed to have installed a camera capturing images of people coming and going from Cawvey Jr.'s residence, and 3) describing an incident where Cawvey Jr.'s spouse was driving fast while passing the message sender. In a message, the sender threatened to run the spouse off the roadway.
- e. After Cawvey Jr. told his father (Cawvey Sr.) about the messages, Cawvey Sr. began to come to RAP to meet with Cawvey Jr. and Alldredge. Shortly after

this, Cawvey Sr. also began to receive similar harassing/threatening text messages on his personal phone from an unknown person(s) from multiple different phone numbers.

- f. After Alldredge began to receive similar messages on his cellular phone, he contacted his wireless provider, Verizon, and had his phone number changed. On or about the same date of the number change, Alldredge began receiving text messages on the new number. The messages, sent from an unknown person(s), indicated they knew Alldredge had changed his number.
- g. On or about May 19, 2020, LEFEBVRE reported to Cawvey Jr. that he too began receiving text messages on his cellular phone from an unknown person(s) asking if it was “Brad” (LEFEBVRE’s first name is Bradley).
- h. Alldredge received messages indicating the person hacked into the business EBay account, responded to customer messages on the account and deleted other messages from customers. Alldredge was able to access the EBay account and found this was all accurate.
- i. Several times, the person(s) sending the messages to Cawvey Jr. and others claimed responsibility for physical damage to things within the business including the Internet connection along with the theft or movement of small items of property within the business. When Cawvey Jr. and/or Alldredge would check those areas, they found items moved or missing. The items included small engine parts and cleaning products.



- j. On or about May 18, 2020, Cawvey Jr. received a text message from this unknown person(s) referencing events at a party Cawvey Jr. attended 10-15 years ago. The messages correctly identified events that occurred at the party.
- k. Cawvey Jr. reported the threats and harassment from the unknown person(s) were coming in the form of text messages from multiple different numbers. Sometimes he would receive multiple messages over the course of more than one day from the same number and often he would receive multiple messages from different numbers on the same days or multiple days in a row. The messages were being sent almost daily. Among the threats/harassment were the following topics and threats:
  - i. Report that Cawvey Jr's spouse was driving too fast and passed the person/persons sending the messages. The person/persons threatened to run the spouse off the road if it happened again. Cawvey Jr's spouse did not recall any specific incident like this,
  - ii. Threats to break into Cawvey Jr's private residence, tie Cawvey Jr. up, molest his minor children, rape his spouse, then make them untie Cawvey Jr. after the assault,
  - iii. Threats to shut off the business Internet at RAP, and after times when the Internet had stopped working, the person/persons have taken responsibility for shutting it down,

- iv. The person/persons have claimed responsibility for stealing items from the business,
  - v. The person/persons have claimed they can monitor the business work areas visually and by audio and have correctly identified events and conversations which took place within the work area when only a few individuals were present including Cawvey Jr, Alldredge, and LEFEBVRE,
  - vi. Threats to commit sexual assault against members of Cawvey Jr's family and throw his spouse into a pond,
  - vii. Expressed a desire to put RAP out of business and/or take Cawvey Jr's position at the business,
  - viii. Correctly identified a time when Cawvey Jr's spouse was home alone –her vehicle was parked in the closed garage and not visible from the roadway,
  - ix. Correctly identified that Cawvey Jr. placed Wifi-connected security cameras at his private residence.
1. During the interview, Cawvey Jr. provided me with paper copies of screen shots he took from the text messages sent to himself, Cawvey Sr, and Alldredge from March 16, 2020 to the day before the interview.

7. Following the interview with Cawvey Jr, I reviewed the text messages he provided that were sent to his personal cellular phone. Some of the content of the messages included:

- a. On or about March 16, 2020: *"LMAO LOL I SEEN U DRIVING TODAY DAM BRO CUT YOUR FUCKING HAIR BUD U LOOK LIKE A FUCKING CLOWN HAHA." [...] U WANNA GEZ FUCKED TONITE. WHAT? YO. WIFES A SLAM PIG N U R KIDS R TRAMPS WAT NOW BITCH." [...] CANT WAIT TO FUCK U IN THR SHOWER WITJ NO MOTHER FUCKING COMDOM ON N A PAPER BAG OVER YOUR HEAD OK. IS THE LITLE SLUT WORK TONITE. ANSER ME. I M ASKING IF THE LITLE SLAM PIG IS GOJNG TO BE HOME TONITE BECAE SHE CULD WATCH THE LITLE TRAMPS WHILE U N I DO OUT FOR A BURN RIDE N PULL OVER SO I CAN FUCK U R TIGHT ASS."*
- b. On or about March 25, 2020: *"MORN FAG SEAN U THIS MORN BY SHIT PLANT BAGAHAHS U DO YOU LOOK LIKE S FUCKEN CLOWN SUCK TO BE U I FELL SORRY FOR YOU R LITTLE TRAMPS BEING A MIX OF U N HER POOR THINGS ANY WAY HAVE U BEN TESTED FIR COVID19? ITS PEPE LIKE U I DO WISH WULD GET IT SND DIE FROM IT. FUCK U." [...] I KNOW MORE THAN U THINK I DO BAHAAAAHA. [...] ITS IN U R SLUTS PLACE OF WORK. WIFES A SLAM PIG. I WULD FUCK HER AGAN. [...] SENSE WEN DID U GET A POOL? LOOKS BEAUTFUL. SUCH A NICE LITLE VIEW. [...] IF U BLOCK ME ONE MORE TIME I WILL*

*SOREAD A RUMOR U MOLEST YOUR CHILDREN DON'T FUCK EITH ME. [...] WANT ME TO SUCK U COCK WAT TIME DOSE SLUT GET HOME BEN DRIVING BY FOR PAST 3 HOUR MITE HAVE TO GO PEEK IN GARAGE."*

- c. On March 26, 2020: *"...I JEST DRIVE BY U HOUSE I SEE THE SLUT S HOME."*
- d. On March 27, 2020: *"I M REALY SURPRISE MATTHEW ALDRICH IS STIL PUSHING TO RUNN THAT BUSINESS CONSIDERED THAT U R SLAM PIG WIFE WORK S IN THE CORRECTIONAL FACILTY WITH THOUSANDS OF INMATES WHO MIT BE INFESTED WITB COVID19[...]BECAUSE I KNOW U WILL NEVER CATCH ME EVER SCUMBAG DO U SEE A ROAD OUT U R WINDOW IV WATCH U MANY TIMS FROM THST ROAD I HAV SEN THE DUDE SMOKEING N THE OKD MAN STAND BY A DOOR MANY TIMES I HAVE BEN WATCHING U N U R FANILY FIR SOME TIME NOW PAY BACK IS A BITCH N IM THE BITCH THAT DON T BACK DOWN SO LOOK LIKE U R GOING DOWN HAHHAHA."*
- e. On or about March 30, 2020: *"...IS IT ALRIZE IF I GO OVER N PLAY WITH U R LITTLE GIRLS I WON T BE MEAN I CAN PLAN BARBIE DOOLS WITH EM I WIL EVEN BRING MY OWN OK I M ALMOST TO U R HOME NOW. [...] U R POOL COVER OR SOME THING IS SINKING THAT CAN*

*CASE THE SIDES TO COLAPSE TRUST I VE BEN THER DONE THSZ  
THAZ IS WHY I GOT RID OF MY POOL WAS TO EXPENSE TO KEEO  
REPAIR ING”*

f. On or about March 31, 2020: *“I GOT GAME CAMS SET UP BY U R  
DRIVEWAY BRO JUST WATCHING OUT FOR YOU I WANT TI MONITOR  
EACH PERSON THST COME TO FUCK U R WIFE N U ALSO I JUST GOT  
DINE SETTING INE UO AT LYOMS DRIVE NOT TO CLOSE TO THR  
HOSE BUT CLOSE ENOUHH I CAN MONITOR VIDITORS. [...] BE  
LOOKMG OUT U R WINDOW TONIGHT AROJND 1230 I I WILL DRIVE  
BY N LITE EM UP FOR U N SHOT MY GUN TO WAKE U R FUCKING  
TRAMPS N THE SLUT TELL HER I WILL FUCK HER TOMORROR IF SHE  
WANTS IT AGAN BRO U R SO DUMB I BEEN FUCKING U R WIFE FOR  
SOME TIME.”*

g. On or about April 10, 2020: *“LET ME TELEL U SCUM IF U R CUNT BAG  
WIFE EVER PASS ME AGAN AT THAT RATE OF SPEED N GEZ THAT  
CLOSE TO MY FUCKING TRUCK AGAN I WILL I STATE I WILL CHASE  
HER DOEN N I WILL I STATE I WIL RUNN THE CUNT OF THE ROAD  
THER IS NO FUCKING NED TI DRIVE LIKE AN ASSHOLE LIKE THAT  
EVER UNLES ITS LIFE OR DEATH N IT MAKE ME LAUG THAT SHE  
DRIVE ARUND N STYLE WITH NICE CAR N U ROLL AROJND IN THSZ  
SHIT BIX TRUCK.”*

- h. On or about April 13, 2020: *"I WILL ESPLANE TO U NOW. U R KARMA IS U R DAUGHTER [minor child's name] U THINK SHE WAS BORN WITH HALF A LEG FOR NO REASIN NO ITVWSS BECAE OF THE ASSHOLD U USE TO BE TO OTHER NOW U HAVE TO DESL WITH HER GETTING PIVK ON N U HAVR TI DEFEN HER. MAKES IT EASIER FOR U RITE THAT HALF A LEG U HAV TO HOLD UP WEN U R FUCKING HER RITE. LISEN TO ME HO MO I DO NT THINK U R TAKIN MY SEROUS I M WATCHING U N I HAVE BEN I M GOONG TO FALLOW U THIS MORNING I BEN BY U R HOME 3 TIMES NOW."*
- i. On or about April 20, 2020: *"ROGER CAWVEY?"*
- j. On or about April 21, 2020: *"BY THE WAY I FORGOT TO TELL U LOLOL THE FRIEND I BROUT WITH ME TO U R PLACE HAS COVID 19 WERE IS U R FUCKING MASK N GLOVES IDIOT LOLOL I HAD HIM WIPE HIS SPIT ON ARM OF U R CHAIR TABLE DOORS U ALL SHULD BE TESTED N U R FAT DAD IS TOUCHING MY OWN SHIT NOW HAHA TOLD U STAY HOME. IM GOIN TO BROKE INTO U R SON JOHN HOME TIE HIM UP SIT HIM DOEN N OPHYSICALLY MOLEST HIS KIDS WILE HE WASHES THEN I WILL RAPE HIS UGLY WIFE THEN LEVE N SHE CAN UNTIE HIM OK. I SEND THIS TO U R BIG FAT DASDY."*

- k. On or about April 22, 2020: *"U SCUMS THINK U GOT IT ALL FIGER OUT WELL NEE FLASH U DON'T I DID 3 THINH LAS NITE ONR WAS INTERNET FOR U N 2 OTER THINGS NO ONR HAS NOTICR YET."*
- l. On or about April 27, 2020: *"OK THIS SHIT GETN BAD IM WORRY DOUBLE D IS PLANING TO SHOOT AT U R WINDOWS TODAY HE IS JUS TRYING TO SCARE U WEN GLAS SHATTERS ALL OVER U I M WORRIED WAT IF HE HITS U I DID T WANT TI SEE ANY ONE HURT I TOLD HIM ITS NOT A GOOD IDEA HE SHULD JUSZ QUIT OR FINE SOME THING ELSE TO DI HE SAID NOT TO WORRY HE HAS GOID AIM HE WINT HIT U MAN JUSZ BE VERY CAUSTIONS TODAY PLESE."*
- m. On or about May 13, 2020: *"I JEST WANTED TO TEL U DOUBLE D SAY THANK U FOR THE VAULR SPRING COMPRESERS [...] HEY BABE FINE OUT HOW AIR PUMP IS RUNING TODAY LOLOLOL. [...] LOVE HOW U IDIOTTS THINK I M IN TO U R CELL PHONES WOW DUM FUCKS I CSN STILL SEE N HARE U DUM ASS."*
- n. On or about May 14, 2020: *"THER U R OFICIALLY ON GRINDR LOOKING FOR A NSA HOOKUP I HAVE POSTED THE ADDRES AS 247 SULLIVAN STRET OUT BACK COME IN FRONT MAIN DOIR ASK FIR ROGER. GAY BOYS COMING OVER TO SEE YOU LOLOL HOPE YOUR HORNEY."*
- o. On or about May 15, 2020: *"I HOPE YALL DID NT PAY TO MUCH FOR CAMERA SYSTEM BECAE I ALREADY CAN DESTROY THEM FASTER"*

*THEN U PUT UP SCUMBAG FIRST I CRASH U R INTERNET PHONE  
MODEMS THRN COME IN AND FIND THR CAMERA DRIVER  
DISCONNECT TAKE IT AND DISPOSE OF PROPERLY AS FAT MATT SAY  
THEN COM MINDSY MORNINF IT IS U R OPOBLEM TO HABR INFINITX  
COME REPLACE THR INTERNET N PHONE MODEM.”*

- p. On or about May 18, 2020: *“REMEMBER WEN U THOT THAT GUY WAS  
TRUNING TI GET WITH U R GIRL N U WHIP OUT U R COCK ON STAGE  
LOLOLOL IT WAS SO SMALL N CUTE U HAVE MORE HAIR THEN U DO  
A PENIS LOLOL I WULD OF SUCK IT ANY WAS I WANT U TO CUM  
DOEN MY THROT OK I STIL BERY HORNY FIR U N I WANT TO FUCK  
HOP ALONG SO BAD I BEEN WATCHING HER SINVE SHE WAS 6 NOW  
SHE MUST BE OLD ENUFF TO BREED RIGJT I CANT WAIT TO MAKE S  
BABY WITH HER N U CAN BE GRANPA IF ONLY U HAD FUCKED ME  
WEN I WANT U TO WE WULDNT BE HAVING THJS PROBLEM RITE  
NOW.”* This text message seemed to reference an incident at a party 10-15  
years prior when Cawvey Jr. became intoxicated and exposed his penis to a  
crowd of people. Additionally, one of Cawvey Jr.’s minor children was born  
with a birth defect to their leg or foot. Cawvey Jr. believed that the  
person/person sending the message was referring to his minor child as “HOP  
ALONG.”

- q. Also on or about May 18, 2020: *“THANKS BABE FOR INSTALING CAMERA  
AT U R HOUSE N THANK U FOR USING WIRELESS LOLOLOL I WISH I*



*HAD WENT BY N SCAN ALONE TIME AGO NOW I CAN WATCH U IN U R HOME N TELL WEN U LEVE N WHEN U COME HOME[...] U R [minor child's first name] IS SO TASTY LOOKING CABT WAIT TO SNATCH HER UP. IMAGINE COMING HIME FROM A LOMG STRESFIL DAY AT WORK N FIND ME ON THAT COUCH BALLS DEEP IN [minor child's first name] ASSHOLE N HER SCREAMING FEEL SO GOOD DADDY. DONT GEZ ANGRY JUST IMAGINE ME FUCKING U R OWN UGLY KID N U WALK IN N CATCH US ON THR COUCH I WILL THEN SAY U CAUGHT ME RED HANDED SLEEPING WITJ U R LITTLE GIRL PISTURE THIS WE WERE BOTJ BUTT NAKED BANGING ON THE SOFA I WILL THEN SAY IT ALRIGHT IT WASN'T ME LOLOLOL."*

- r. In addition to the text within the messages, there were several images depicting nude sexually aroused men and men ejaculating.

8. I also reviewed messages Cawvey Jr. provided which were sent to his work cellular phone. The messages were similar in content and style when compared to Cawvey Jr.'s personal phone. Some of the messages included the following:

- a. On or about April 15, 2020: *"ONE OF THE DAYS I M GONIN TO BROKE INTO U R HOME I DON T CARE WAT SECRETY U HAVE N I M GOIN TO TIE U UP N MOLEST U R DAM WIFE OK N ULL HAV TO WATCH IT N I ALRDY KNOW WEN U R WIFE SEE THIS COCK SHE WIL LOVE IT N ULL HAVE TI WATCH HER GEZ OFF RIDING ME BAREBACK."*

- b. On or about April 23, 2020: *IM GOING TO RAPE U R FAMILY TODAY CANT WAIT. YES RAPE THE KIDS TO. I WAS IN SIDE AGAN LAST NITE I DON T WANT TO SEE NO ONE PISICALLY HURT SO PLEASE DO NOT TURN ON THE GAS UNTIL U CHECK OVER GAS LONE LOLOL.”*
- c. On or about April 24, 2020: *“HEY TOGER I M GOING TO RAPE U R UGLY LITTLE GIRLS N RAPE U R SLUT WIFE N TROW HER BODY IN A POND. U R WIFE WILL LOVE IT. [...] IM WASHING U AT U R DESK. PULL OUT U R COCK RITE NOW.”*
- d. On or about April 28, 2020: *“DID U C I DELETE A LOT OF U R EBAY MESSAGE YESTERDAY? LOLOL. [...] I M GOING TO RAPE U R KIDS START WITH [minor child #1’s name] THEN [minor child #2’s name]. [...] I MADE U AN ACOUNT ON GRINDR I PIT THE ADRESS AS 247 SULLIVAN STREET BACK SIDE WERE BLUE CHEVY IS GO IN THSZ DOIR.”*
- e. On or about April 30, 2020: *“NICE PISTURS ON THE SD CARDS BY A WAY LOLOL I WAS GOKKG TO TAKR THE HOLE UNIT TILL I DECIDE I DID T HABE A NEDD FOR BIG THINGS I LIKE BUTON SIZE BATERY SMALL ONE NICE NEW LOCK SET TO BAD I DON T COME IN THAZ WAS LOLOLO.”*
- f. On or about May 5, 2020: *“I WILL RAPE U R KIDS THEN MERDER RHEN.”*

9. On or about June 2, 2020, I interviewed Cawvey Jr. by telephone. He reported the harassing/threatening text messages stopped on or about May 18, 2020.

10. On or about June 11, 2020, I interviewed Cawvey Jr. by telephone. He reported the following:

- a. The harassing/threatening text messages began again. On or about June 9, 2020, he received a text message from an unknown person(s) which referenced switching the butterflies. At first, Cawvey Jr. did not know what this meant. On or about June 11, 2020, Cawvey Jr. checked the butterflies of several carburetors (engine parts) within RAP and found the carburetor butterflies had been removed and replaced with different parts.
- b. Also, on or about June 11, 2020, Cawvey Jr. received several text messages on his personal and work cellular phones from an unknown person(s). The messages referenced a private conversation he had with Matthew Alldredge on the morning of June 11, 2020 inside RAP about the installation of surveillance cameras. Bradley LEFEBVRE was the only other person present for this conversation which occurred within several different areas of the business throughout the morning.

11. On June 16, 2020, I interviewed Cawvey Jr. by telephone. He reported the following:

- a. On June 12, 2020, he received a text message from an unknown person(s) about a music speaker within the RAP business. Cawvey Jr. checked the speaker and found the foam around the speaker had been cut.
- b. Also, on June 16, 2020, Cawvey Jr, Alldredge, and LEFEBVRE began installing video surveillance cameras within the business. LEFEBVRE was in the ceiling or attic of the business installing a new cable to power one of the cameras. Later that same day, LEFEBBRE reported he received a text message from an unknown person(s) on his cellular phone. The message indicated that LEFEBVRE almost caught the person in the attic space. The person indicated they were hiding in the attic space, next to a black heating duct. The person also indicated they cut the end of the camera wire and tied it to a conduit cable within the attic.
- c. Cawvey Jr. and Alldredge later inspected the attic and found a hole in the wall between their attic space and the attic space of a neighboring business along with the camera power cable tied to a conduit cable. During this time, Alldredge fell off a step ladder and was transported to the hospital by ambulance. The unknown person(s) later sent text messages to Cawvey Jr, Alldredge, and LEFEBVRE about Alldredge's injury and used language referencing Humpty-Dumpy having a large fall.
- d. On June 15 and 16, 2020, Cawvey Jr. and LEFEBVRE both received text messages from an unknown person(s). The messages referenced burning down

the business, cutting propane lines, taking over the workspace, and getting the business to move.

12. On or about June 19, 2020, I interviewed Cawvey Jr. by telephone and he reported the following:

- a. On June 16 or 17, 2020, he, along with LEFEBVRE, were speaking in the parking lot of RAP. Two unknown males were parked in a truck within the same parking lot. Cawvey Jr. felt the males were watching them. After Cawvey Jr. returned inside the business, he checked his cellular phone and found text messages from an unknown person(s) that talked about going for a ride in the truck and having a “circle jerk.” Cawvey Jr. told LEFEBFRE about the messages and LEFEBVRE reported receiving similar messages about getting in the truck to “ride-bitch.”
- b. On or about June 18, 2020, Cawvey Jr. received text messages on his personal cellular phone from an unknown person(s) indicating that person(s) created a fake profile for Cawvey Jr. on the Grindr Application. Cawvey Jr. was aware that Grindr was primarily used as an online dating application for homosexual men. The unknown person(s) warned Cawvey Jr. that men would start showing up at the business for dates and/or sexual relations with him.
- c. During the day on June 18, 2020, four different men arrived at the business asking for Cawvey Jr. and/or LEFEBVRE. All four men reported setting up dates for sex on the Grindr Application.

- d. LEFEBVRE created a Grindr profile so he and Cawvey Jr. could view the fake profile the men were responding to. LEFEBVRE and Cawvey Jr. discovered a profile under the name “Roger Cawvey” that included a profile photograph of Cawvey Jr.’s personal vehicle parked outside of RAP. There was also a paragraph description indicating users should come to the business address to have homosexual relations with Cawvey Jr. and LEFEBVRE. LEFEBVRE took screen shots of the fake profile on his cellular phone. Cawvey Jr. contacted Grindr to report the abuse and the profile was deleted.

13. On or about June 30, 2020, I interviewed Cawvey Jr. by telephone. During the interview, Cawvey Jr. reported the following:

- a. Cawvey Jr. learned through a series of other people that the person responsible for the text message harassment/threats might be LEFEBVRE among several others. According to the information provided through several people, LEFEBVRE had a history of this type of behavior, including harassing a female who previously employed his girlfriend.
- b. Further, Jason LaRochelle<sup>1</sup> shared a screen shot with Cawvey Jr. of a text conversation between LaRochelle and LEFEBVRE in which LEFEBVRE confessed that he had harassed an older woman in New Hampshire through Facebook.

---

<sup>1</sup> Jason LaRochelle is Matthew Alldredge’s son-in-law. LaRochelle communicates with Cawvey Jr. semi-regularly. He is receiving similar harassing messages from an unknown person(s).

- c. Alldredge told Cawvey Jr. that he found a receipt for a \$50 pre-paid cellular phone card in a business work truck that LEFEBVRE was known to drive.  
Alldredge did not save the receipt and did not remember the information on it.
- d. During, or just prior to, the weekend of June 27-28, 2020, an unknown person(s) sent text messages to Cawvey Jr. indicating homosexual men would be arriving to Cawvey Jr.'s private residence for sex acts. On or about June 27, 2020, three different men arrived at his house. He confronted each man. Two of the three men admitted they responded to a Grindr profile post directing them to the address. Using a Grindr account which he created to investigate these actions, Cawvey Jr. found a fake profile without a photo or description. The profile was labeled "Looking" or "Seeking." Users could then communication through private message with other users in the area. Cawvey Jr. reported the abuse to Grindr.
- e. Cawvey Jr. captured screen shots of the fake account profile. He also noted that the Grindr app indicated that the device using the fake profile was 10 miles away from him.
- f. After these three men arrived and departed his residence, Cawvey Jr. contacted the Springfield Police Department. An officer responded and after Cawvey Jr. described the situation and talked about his employment and co-workers, the officer told him it was likely Bradley LEFEBVRE and Noah Dailey who were responsible for sending the threatening/harassing text

messages. The officer reported LEFEBVRE and Dailey were suspected of similar conduct during a Springfield Police investigation.

- g. After the police officer left Cawvey Jr.'s residence, Cawvey Jr. drove to LEFEBVRE's residence in Springfield, Vermont to talk with him. Cawvey Jr. did not let on that he suspected LEFEBVRE could be responsible. While there, Cawvey Jr. learned that Dailey, who also lives with LEFEBVRE, was working at Tractor Supply. Later the same day, Cawvey Jr. drove to Tractor Supply in Claremont, New Hampshire and saw Dailey's vehicle in the parking lot.
- h. In mid-June of 2020, Cawvey Jr. and Alldredge installed a video surveillance system at RAP. There were two cameras outside and several cameras inside the business. The cameras connected, via wire, to a digital video recorder ("DVR") located inside the office break room area. For several nights while the system was being installed, a longtime friend and former co-worker of Alldredge, Bruce Deuso, provided overnight security at RAP. LEFEBVRE, Alldredge, and Cawvey Jr. were all aware Deuso was providing nighttime security.
- i. On or about June 18, 2020, Cawvey Jr. was in the process of welding a security box to store the DVR system. LEFEBVRE came to Cawvey Jr. and told him Alldredge thought someone was on the roof of the business. Cawvey Jr. quickly ascended stairs and/or a ladder leading to the roof while



LEFEBVRE remained at the base of the stairs or ladder. After several minutes of searching, Cawvey Jr. did not locate anyone on the roof. When he returned into the business, LEFEBVRE was waiting in the break room where the DVR system was being stored.

j. Cawvey Jr. returned to working on the security cabinet and DVR and he discovered the DVR system had been damaged. It appeared someone had placed a screwdriver or similar object into the HDMI port of the DVR and damaged it.

k. Cawvey Jr. later received a text message from the unknown person(s). They claimed responsibility for damaging the DVR.

14. Using Google Earth Pro –an open source commercial software program with world-wide mapping capability, and a program I have found reliable in the past –I checked the distance between Cawvey Jr.’s residence and Tractor Supply. I found the distance was about 10.24 miles whereas the distance between Cawvey Jr.’s residence and the residence where LEFEBVRE and Dailey reside, 20 Lewis Street, Springfield, Vermont, was slightly over one mile.

15. On or about July 1, 2020, I interviewed Cawvey Jr. by telephone. He advised of the following information:

- a. Alldredge told Cawvey Jr. that Individual #1<sup>2</sup>, an associate of Alldredge, received a text message from LEFEBVRE claiming responsibility for setting up the Grindr profile and sending the men to Cawvey Jr.'s residence. I later obtained from Individual #1 screen shots of the message between Individual #1 and LEFEBVRE. The text message was sent from the number (802) 952-9253 and read, *"I sent 4 gays to jr house Saturday he was so mad he came over cuz he couldn't be home any more. He pulled a gun on one of them then called the cops and told them he almost shot someone."* The contact was saved in Individual #1's phone as, "Do Do."
- b. Cawvey Jr. confirmed LEFEBVRE's phone number was (802) 952-9253.
- c. I checked the phone number using [www.zetzi.com](http://www.zetzi.com) –a website I have used in the past to find the wireless carrier of phone number and found to be reliable – and determined (802) 952-9253 was an AT&T number. The website also indicated the number was registered to Bradley LEFEBVRE.
- d. During a prior conversation with Jason LaRochelle, he told Cawvey Jr. that LEFEBVRE admitted he was responsible for sending the text messages to Cawvey Jr. in 2018 after the Christmas party where Cawvey Jr. had too much to drink.

---

<sup>2</sup> Individual #1's identity is known to the FBI; they are not a confidential informant. Individual #1 cooperated with the FBI during this investigation and asked their identity be kept private from the public. Individual #1 was not made any promises, paid any money, or threatened with prosecution in exchange for their cooperation. Individual #1's criminal history reports a misdemeanor theft of services conviction in 2013.

- e. Alldredge also told Cawvey Jr. that his daughter, Danielle Alldredge – who is dating LEFEBVRE, has children with him, and lives with him –has seen LEFEBVRE and Dailey in possession of multiple cellular phones at their residence, 20 Lewis Street, Springfield, Vermont.

**INDIVIDUAL #1 INTERVIEW/INFORMATION**

16. On or about July 9, 2020, I interviewed Individual #1 in Springfield, Vermont.

Individual #1 told me the following information:

- a. Individual #1 has known LEFEBVRE for about 12 years. Individual #1 is occasionally employed at RAP with LEFEBVRE and has regular contact with him via cellular phone.
- b. LEFEBVRE brags to Individual #1 that he harasses people through text message and phone calls. LEFEBVRE pretends to be different people and/or remains anonymous. LEFEBVRE uses the TextNow app on a pre-paid cellular phone to send harassing text messages to people he does not like. LEFEBVRE has at least two cellular phones. One phone is a post-paid AT&T cellular phone on a contract. He uses that phone for everyday use; the number is (802) 952-9253. The other phone is a pre-paid phone that Individual #1 believed was on the Verizon cellular network. Individual #1 does not know the phone number of the pre-paid phone. LEFEBVRE purchases \$50 pre-paid phone cards to use this phone. Once, LEFEBVRE purchased a phone card at Walmart and left the receipt in a RAP work truck. LEFEBVRE has talked

about connecting the pre-paid phone to his AT&T phone's mobile hotspot in order to connect to the Internet and send messages to people. LEFEBVRE always has both phones with him and usually carries the pre-paid phone in his back pocket. One phone is in a black case, the other is in a green-colored Otterbox case. The pre-paid phone might be an Apple iPhone, but Individual #1 was not positive.

- c. For several months, Individual #1 has communicated with LEFEBVRE about Matthew Alldredge. Individual #1 lives with Alldredge. LEFEBVRE asks Individual #1 questions about Alldredge's work schedule and activities. Individual #1 assumed LEFEBVRE was asking because Alldredge was the boss at RAP and LEFEBVRE would want to know when the boss was coming to work. Individual #1 later became aware that LEFEBVRE was using this information to harass Alldredge after Alldredge told Individual #1 he was getting harassing text messages about being followed to work. Individual #1 believed that LEFEBVRE was using the information Individual #1 provided to LEFEBVRE to stalk and/or harass Alldredge.
- d. Individual #1 consented to a search of their cellular phone. The search revealed numerous text messages between Individual #1 and a contact saved as, "Do Do," who Individual #1 explained was LEFEBVRE. The contact, "Do Do," has cellular phone number (802) 952-9253.

- e. Recently, LEFEBVRE sent Individual #1 a text message in which LEFEBVRE admitted that he sent five homosexual men to “Jr’s” house over the weekend. “Jr” pulled his gun on one of them and almost shot the male. Individual #1 identified “Jr” as John Roger Cawvey Jr. Individual #1 was concerned that Cawvey Jr. might shoot someone and get in trouble, so Individual #1 told Alldredge about the messages and sent Alldredge a screen shot of the message LEFEBVRE sent Individual #1.
- f. LEFEBVRE has also bragged to Individual #1 about harassing Stuart Beam. LEFEBVRE has sent harassing text messages to Beam and made harassing phone calls to Beam while disguising his voice. LEFEBVRE once convinced Beam to cut down some trees at a hotel/motel in Bellows Falls, Vermont. LEFEBVRE pretended to be the property manager or owner and told Beam he would pay him after the work was completed. After Beam cut some of the trees, he found out it was a hoax and turned himself into the local police<sup>3</sup>. He was almost arrested for trespassing and vandalism. LEFEBVRE also harasses Beam by sending him messages about stealing his chickens and a tractor from Beam’s property.
- g. Individual #1 also knew that LEFEBVRE maintained three fake Facebook accounts. One was under the name, “Chelsea Goodrich,” another was under

---

<sup>3</sup> I was unable to locate any police reports related to this incident.

the name, "Ronnie Watkins," and the third was under the name, "Jessica Fletcher."

17. I later reviewed the text messages between Individual #1 and LEFEBVRE. The messages included questions and/or statements from LEFEBVRFE such as:

- a. *"So what time will he be leaving,"*
- b. *"Does Matt and Cyndi go in [the pool],"*
- c. *"Is he still there,"*
- d. *"Did he leave,"*
- e. *"I'd love to go to jrs house and do target practice with the ar on his truck and 968"*
- f. *"Did he go to office this weekend,"*
- g. *"So they didn't do cameras,"*
- h. *"I'm back where phones are,"*
- i. *"Stuart just fucken called me,"*
- j. *"Jr has the stupid cams set up again I shut those mother fuckers off,"*
- k. *"Can't even text when he gets here cuz he always catches me,"*
- l. *"He set up game cameras,"*

- m. *"Can't believe Bruce stayed the night lol,"*
- n. *"What's Matt doing,"*
- o. *"He leave yet or just getting ready,"*
- p. *"Pranker told him he very lazy man [photo of Stuart Beam attached],"*
- q. *"Wonder if the cameras are working,"*
- r. *"I sent 4 gays to jr house Saturday he was so mad he came over cuz he couldn't be home any more. He pulled a gun on one of them then called the cops and told them he almost shot someone [...] I don't feel bad what I'm doing to jr he deserves everything he gets for what he did to you and how he acts towards me here."*

**RECORDED/MONITORED PHONE CALL WITH LEFEBVRE**

18. On July 15, 2020, Individual #1 placed a recorded and monitored phone call to LEFEBVRE at (802) 952-9253 to obtain evidence during this investigation. I was present with Individual #1. I observed Individual #1 call the number (802) 952-9253, saved as, "Do Do" in Individual #1's phone, monitored and recorded the call. During the call, LEFEBVRE asked if "Matt" left the house. Individual #1 told LEFEBVRE that "Jason" was complaining about getting calls. LEFEBVRE inquired if "Jason" was yelling about it. LEFEBVRE also stated that "Jr" and his dad are weird. During a portion of the call, the recording equipment failed. It was during this time that LEFEBVRE and Individual #1 discussed Stuart Beam and an incident where Beam unlawfully cut trees at an abandoned hotel/motel in Bellows Falls, Vermont.

LEFEBVRE told Individual #1 that he convinced Beam to cut the trees or he (LEFEBVRE) would lose the contract with the town manager. LEFEBVRE also spoke of a woman from Texas who was suing people for damage done to the hotel/motel. LEFEBVRE stated he told the woman that Beam was responsible for cutting the trees and the woman was now going to sue Beam.

### **SEIZURE OF FIVE CELLULAR PHONES**

19. On July 9, 2020, Cawvey Jr. discovered five cellular phones and some paperwork associated with cellular phones hidden on a shelf under a work bench within the RAP business. This work bench was in an area used to clean auto parts. LEFEBVRE used the area when he was at work. Cawvey Jr. photographed the phones and left them in place.

20. On July 15, 2020, I met with Cawvey Jr. and seized the phones and paperwork described above. I found the five cellular phones and two paper documents associated with cellular phones on a knee-high shelf below a work bench within the RAP work area. The phones are described as follows: 1) a black "TCL" phone with no visible markings, 2) a black "ZTE" phone with no visible markings, 3) a black Apple iPhone 8 Plus (A1897), 4) a silver Apple iPhone 5S (A1533) in a green and black case, and 5) a black Asus Android phone, model V520KL. Among the phones was a "Quick Start Guide" for one phone, and paperwork for a TracFone listing an IMEI and SIM number. Cawvey Jr. recognized two of the phones were old phones owned by RAP (including the Apple iPhone 5S in a green and black case) while two of the phones likely belonged to LEFEBVRE because Cawvey Jr. did not recognize them.



**RECORDED/MONITORED MEETING WITH LEFEBVRE**

21. On July 22, 2020, Individual #1 met with LEFEBVRE in person at RAP, 247J Sullivan Street, Claremont, New Hampshire. The meeting was planned and recorded by the FBI. Prior to the meeting, I met with Individual #1 and provided Individual #1 with covert electronic surveillance equipment in order to audio and video record the meeting. Individual #1 was surveilled by law enforcement as Individual #1 arrived at RAP. Following the meeting, Individual #1 was surveilled by law enforcement traveling to a predetermined location. I retrieved the covert electronic surveillance equipment from Individual #1. The following information was gained during the meeting as a result of interviewing Individual #1 and reviewing the audio recording:

- a. When Individual #1 arrived at RAP, only LEFEBVRE was present. A truck registered to LEFEBVRE was parked outside the loading dock area. The truck was a white colored Ford truck with Vermont registration 342A870<sup>4</sup>. Near the end of the recording, a male believed to be Alldrege and a male believed to be Cawvey Jr. were heard speaking<sup>5</sup>. The recording ended shortly after.
- b. When Individual #1 first arrived at RAP, Individual #1 began speaking with LEFEBVRE. The voice characteristics were unique and sounded to be the

---

<sup>4</sup> A Vermont Department of Motor Vehicle record check revealed that the license plate was assigned to a 1993 Ford Truck, color yellow, and registered to Bradley L. LEFEBVRE of 20 Lewis Street, Springfield, Vermont. The vehicle the registration plate was attached to was white in color and appeared to be a later model Ford truck.

<sup>5</sup> I later spoke with Cawvey Jr. and he reported (as confirmed by physical surveillance) that both he and Alldredge arrived at RAP while Individual #1 and Lefebvre were meeting.

same person Individual #1 spoke to during the July 15, 2020 recorded telephone call.

- c. LEFEBVRE discussed cameras inside RAP and the only spaces of the business' interior which were not captured by cameras. LEFEBVRE acknowledged this was the area he went to send text messages. LEFEBVRE said he was not sure which cameras work and that "Jr" and "Matt" were so secretive<sup>6</sup>. LEFEBVRE was aware some cameras belonged to RAP because he helped install them. He mentioned a video recorder was now located in "Matt's" office within a locked filing cabinet with locks on both sides. Individual #1 stated, "Guess you're not getting that with a screwdriver, are you?" LEFEBVRE laughed in acknowledgement. Individual #1 spoke rhetorically about having a key, having a screwdriver, and tearing it up. LEFEBVRE asked Individual #1 if "he" read that text message to Individual #1 and Individual #1 said no. LEFEBVRE then stated, *"I told him I can't wait for you to put security in, I'm gonna come over there and hack your Internet, shut the Internet down."* Individual #1 responded, *"Oh, you text him?"* LEFEBVRE stated, *"Yea...go right inside and find that box and destroy it and take cameras with me."*
- d. LEFEBVRE said that someone [*in context, understood to be Alldredge*] changed his phone number twice but told LEFEBVRE about it both times.

---

<sup>6</sup> Individual #1 has reported that "Jr" is Cawvey Jr. and "Matt" is Matthew Alldredge.

- e. LEFEBVRE was heard talking out loud about using a phone, specifically stating that he did not think it was working, he needed to get a new number, and he was not “signed in” yet. LEFEBVRE and Individual #1 discussed “Jason” getting messages about his daughter being fat and how the message sender was asking for naked photos of “Jason.”<sup>7</sup> LEFEBVRE explained he was trying to get “Jason” to send nude photos with his face obscured so that LEFEBVRE could then send those nude photos to “Jr.” Individual #1 asked if LEFEBVRE was “*still fucking with [Jr.]*” and LEFEBVRE responded, “*I haven’t in a while.*”<sup>8</sup>
- f. LEFEBVRE said it was nice without “Jr” around while “Jr” was on vacation<sup>9</sup>. “Jr” would not tell LEFEBVRE where he went on vacation. LEFEBVRE stated he did not like “Big Roger”<sup>10</sup>. LEFEBVRE stated that he and “Matt” started the company but now “Jr” was a partner and received dividends from the business.
- g. LEFEBVRE referenced the day “Matt” fell off a ladder because he was trying to get on the roof to see where the guy got inside. He then spoke about a text

---

<sup>7</sup> Individual #1 reported “Jason” is Jason LaRochelle, Alldredge’s son-in-law. LaRochelle has also been receiving harassing text messages from an unknown person(s).

<sup>8</sup> Cawvey Jr. has not received threatening/harassing text messages from the unknown person(s) since on or about July 14, 2020.

<sup>9</sup> Cawvey Jr. reported to me that he had been out of state on vacation from Thursday-Sunday in the month of July 2020.

<sup>10</sup> Individual #1 reported “Big Roger” is John Roger Cawvey Sr.

message regarding “Matt” being lazy and telling people what to do all the time.

- h. LEFEBVRE said “Stuart” brought a *[political]* sign over to LEFEBVRE’s house the night before<sup>11</sup>. LEFEBVRE told “Stuart” that “Zach” had driven over the sign and “Stuart” called the police. LEFEBVRE spoke to Individual #1 with a disguised voice mocking how he did (or was planning) to call “Stuart” and tell him he ran the sign over. LEFEBVRE mentioned a phone and how “Stuart” told him the Springfield Police have evidence that LEFEBVRE is behind the activity. LEFEBVRE mentioned having a different phone and how he did not want to use that phone.
- i. LEFEBVRE was heard speaking out loud about a phone. He made statements like, *“Oh, wasn’t signed in yet [...] You have been logged out of messenger [...] I remember why I hate this phone.”* LEFEBVRE and Individual #1 discussed getting into “Chelsea’s” *[Facebook]* page because “Stuart” thinks it is “Zach” using a fake Facebook to harass him. Individual #1 asked LEFEBVRE about hiding the phone and charging it overnight. LEFEBVRE acknowledged he did. Individual #1 later told me he saw LEFEBVRE’s “prank” phone was plugged in and charging under the work bench. Additionally, LEFEBVRE was heard saying, *“stuartbeam@gmail.com [...] Don’t use my location [...] 8% [...] Getting numbers.”* Individual #1 reported

---

<sup>11</sup> According to the Springfield Police Department, Beam is running for the political office of State Representative in Vermont.

that LEFEBVRE had downloaded an app called “TextMeNow” or something similar. It sounded like LEFEBVRE was checking the phone multiples times and made comments that the phone was still calling “Stuart” and wouldn’t hang up. Later, LEFEBVRE mentioned a different phone that he did not want to use. LEFEBVRE said he restarted [the phone] and had to log back into Wifi. He commented that he almost brought “the other” phone from home but forgot it.

- j. LEFEBVRE was then heard making a prank call. Another male’s voice could be heard answering the phone call. LEFEBVRE spoke in a disguised voice and referenced running over three of the male’s signs last night. After they seemed to have difficulty communicating over a poor connection, LEFEBVRE told the male he was masturbating and that he would call the male’s house.
- k. LEFEBVRE was then heard making a second call. A female answered. LEFEBVRE spoke in the same disguised voice and told the female he ran three of “Dad’s” signs over last night. He also told the female that [Dad] was his lover, then said, “*Want me to come to your work and fuck you in the bathroom again?*” LEFEBVRE continued a short discussion about sexual activity with the female before the call ended.

- l. LEFEBVRE then made a third prank call. This time, the recipient's voicemail picked up. The voicemail greeting mentioned Stuart Beam and LEFEBVRE was heard mocking the voicemail greeting after he hung up.
- m. LEFEBVRE asked Individual #1 if Individual #1 wanted to call "Stuart" back. Individual #1 stated no and LEFEBVRE referenced that Individual #1 had previously spoken to "Stuart" and offered to bring coffee or donuts to him. The context of that comment was not completely clear; however, it would suggest that Individual #1 was, at one point, involved in harassing "Stuart."

22. Immediately following the recorded meeting between Individual #1 and LEFEBVRE, I interviewed Individual #1 and learned the following information:

- a. LEFEBVRE has been sending the similar threatening/harassing text messages to Jason LaRochelle. LaRochelle is married to Alldredge's daughter.
- b. Individual #1 saw that LEFEBVRE had two cellular phones. One was a personal phone which Individual #1 recognized to be the phone on the AT&T account. The other was a TracFone which LEFEBVRE was keeping under his work bench, plugged in and charging. It was located behind a red-colored medical supply box. The work bench was in an area that all employees use but was a space which LEFEBVRE seemed to work most. This TracFone was the one LEFEBVRE used to send harassing text messages, use fake Facebook accounts such as "Ronnie Wilkins" and "Chelsea," and make anonymous and harassing phone calls from. The phone had a cracked screen. Individual #1

saw LEFEBVRE install a new text messaging application called “TextMeNow” or something similar. When Individual #1 left RAP, the phone was plugged in and charging under the work bench.

**ADDITIONAL PHONE(S) DISCOVERED AT RAP**

23. On July 22, 2020, I spoke with Cawvey Jr. by phone. Cawvey Jr. was at RAP. At my request, Cawvey Jr. checked the work bench area described by Individual #1. It was the same work bench area from which I seized the five phones described above on July 15, 2020. Cawvey Jr. located and photographed a black “Orbic” Android style cellular phone under the work bench. The phone was plugged into power with a black cable and resting next to a red colored first aid kit. Cawvey Jr. sent me two photographs of the “Orbic” phone under the work bench.

24. Near the end of the workday on July 22, 2020, I spoke with Cawvey Jr. and he reported the “Orbic” phone was gone. LEFEBVRE had left work for the day at that time.

25. On or about July 23, 2020, Cawvey Jr. notified me he located another cellular phone on the shelf of the workbench where the five other cellular phones were seized. This phone was a modern smart phone with a black case stamped with a logo reading, “blackweb.” Cawvey Jr. sent me photographs he took of the phone and its location. After LEFEBVRE left work for the day, Cawvey Jr checked the shelf and the phone was gone.

**RECENT TEXT MESSAGES TO CAWVEY JR AND ALLDREDGE**

26. I have subsequently obtained additional screen shots of text messages sent to both Cawvey Jr’s work and personal cell phones. The content of the messages remained similar. The

text messages included admissions that the unknown sender(s) was sending men to Cawvey Jr's personal residence. The last message I reviewed was received on or about June 28, 2020.

27. On July 28, 2020, I reviewed a series of text messages sent to Alldredge from an unknown person(s). Among many of the messages were the following:

- a. On or about June 15, 2020: *"IF I INSTAL THOS TODAY I WILL BE SURE I BURN U R SHIT TO THR GROND [...] TONITE ASSHOLE [...] JUST PACK U R SHIT N GET THR FUCK OUT OF THIS BUILDING U IGNORANT ASSWIPE [...] I HAVE NO PROBAM WITJ HIM U LIER BUT IF U WANT I WIL RAPE HIS KIDS TO HOW U LIKE ME NOW [...] LOVE HOW U MAKE THAT GUY THE FUXKEN BITCH DO THIS DO THAT N U R ALWAYS BITCHEN FOR WJAZ HE DOSE N U N FAG JEST WALK AROUND ALL DAY LIKE LOSS PUPPY DOGS FUCK U U TRET THAT GUY LIKE PESE OF SHIT N KISS ROGER ASS [...] U N THAT GUY START THST BUSNESS TOGETHER BACK IN A DAY N I CALL N ASS FOR A PART N U ESPLAIN IT A FAMLY BUSNES U N U R DAUGHTER N SOM IN LAW THEN U TAKE ON ROGER N HIS FAT DAD N OTHER GUY AINT SHIT [...] WHO FUCK CARE WAT TIME HE COMR IN OR LEVE HE IS U R BITCH ROGER MAKE HIM HELP SHIP ON MONDAX N ASS HIM FOR STUFF ALL DAY LOMG N U U FAT FUCK MAKE HIM CRAWL AROUNF UP TOP N RUSH HIM WHOLE TIMR DO IT YOIR SELF U FAT FUCKING PECE OF SHIT U AINT SHIT [...] IF HE LEFT U THST BUSNES WULF GO TO SHIT FAT FUCK NO INE WOULD START A BUSNES WITH SOMEINR THEN BE*



*STOMPED ON N HAVE SOME OTHRT FAG COME IN AND RUB IN THE  
FACR HE OWN IT.”*

**INTERVIEW OF ALLDREDGE**

28. On or about July 30, 2020, I interviewed Matthew Alldredge to obtain clarifying information. He provided the following information:

- a. After Alldredge began to receive threatening/harassing messages in the spring of 2020, he changed his phone number with his cellular phone provider. The number change took effect at or about 1138 hours. At or about 1208 hours on the same day, Alldredge began receiving text messages from an unknown person(s) stating they knew he changed his phone number. Alldredge provided his new phone number to his wife. Alldredge suspected his wife then provided the new number to their daughter, Danielle, who is in a long-term relationship with LEFEBVRE, and Danielle likely provided the number to LEFEBVRE.
- b. On the date that the DVR system at RAP was damaged –the same date Cawvey Jr. checked the roof for someone –Alldredge and LEFEBVRE both suspected someone was on the roof. Alldredge thought, for quite a few days, that he could hear noises on the roof. Additionally, he remembered that one of the men who arrived at RAP for a Grindr date told them he was supposed to meet the date on the roof. Based upon his suspicion, Cawvey Jr. checked the roof while LEFEBVRE and Alldredge guarded exterior doors at opposite ends

of the RAP warehouse. During this time, LEFEBVRE was the only person who would have had access to the kitchen/break room area where the DVR was located. For that reason, Alldredge suspected LEFEBVRE damaged the DVR HDMI port.

- c. When the surveillance camera power cable was cut and tied to the conduit cable in the attic, LEFEBVRE was the only one in the attic. The attic was a small four-foot space.
- d. LEFEBVRE is a salaried employee who works forty-hours a week Monday through Friday. He has only taken one or two afternoons off from work to attend doctor's appointments within the past several months. Alldredge was sure that LEFEBVRE was at work on March 25-26, 2020<sup>12</sup>.
- e. In or about early April 2020, Alldredge received a text message while he was at or near Walmart. The message indicated he was at Walmart and was riding "Gangster" with the seat tipped back in his vehicle. Alldredge is a larger person and regularly drives with his seat tipped back. LEFEBVRE has driven Alldredge's vehicle before and commented to him about the seat being "Gangster."
- f. The last text message Alldredge has received, to date, was on or about July 7, 2020. The message referenced getting "Jason" to send pictures of his penis to

---

<sup>12</sup> The same dates the TextNow/Pinger app account registrations resolved to the RAP IP address.

the sender, then the final message berated Alldredge for ignoring the messages. On or about the same date, LEFEBVRE told Alldredge that he thought the stalker “wouldn’t bother you anymore.”

**20 LEWIS STREET, SPRINGFIELD, VERMONT**

29. I have established that LEFEBVRE lives at 20 Lewis Street, Springfield, Vermont, a single-family residence, through the following means: 1) According to the Vermont Department of Motor Vehicles, LEFEBVRE lists that as his address, 2) on July 13, 2020, LEFEBVRE was pulled over by VSP Trooper Ryan Miller and issued a written warning for failing to have his vehicle registered. Trooper Miller documented LEFEBVRE’s address at 20 Lewis Street, Springfield, Vermont, 3) on July 22, 2020, the Springfield Police Department responded to a vandalism complaint at 20 Lewis Street, Springfield, Vermont (regarding Stuart Beam’s political sign being damaged, as further described above). As part of the investigation, the officer interviewed LEFEBVRE and he acknowledged being present at the address in the evening on July 21, 2020, and 4) Cawvey Jr. has reported to me that LEFEBVRE lives at that address and he has visited him there recently.

**SUBPOENA RESPONSE**

30. Based upon my review of text messages screen shots provided by Cawvey Jr, I learned that particular phone numbers were used to send threatening/harassing text message(s) to Cawvey Jr’s personal and work cellular phones, and Cawvey Sr.’s cellular phones on particular dates and times. Using open source Internet searches and subpoena compliance, I was able to identify the wireless carrier(s) of those numbers. Most, if not all, of the numbers used resolved to

Internet-based texting or voice over Internet protocol (“VoIP”) services such as TextNow or Pinger. Those services typically capture and retain limited subscriber information such as the account registration date, time, and Internet Protocol (“IP”) address(es). Some of the IP addresses can be traced to a physical location while other IP addresses cannot. Through investigation, I learned the following:

### **TEXT NOW SUBPOENA RETURNS**

31. (802) 347-4164 was used to send threatening/harassing text message(s) to Cawvey Jr’s personal cellular phone on or about March 25, 2020 and the number (802) 278-1053 was used on or about March 26, 2020. Using an open source website, [www.zetx.com](http://www.zetx.com) –a website I have used in the past to identify the wireless carriers of a particular phone number, and found to be reliable –I identified both numbers were assigned to the wireless carrier Bandwidth. I know Bandwidth sells and/or leases phone numbers to 3<sup>rd</sup> party companies. Bandwidth will provide law enforcement investigators with the wireless provider they sell and/or lease the number to without legal process. I contacted Bandwidth and learned both numbers were leased or sold to TextNow, Inc. TextNow, Inc. was served with legal process and later provided subscriber information, including the account registration date/time and IP address used to create the target accounts. The accounts were created on March 25 and March 26, 2020 and the account registration IP address was “73.68.213.55” for both accounts. Using an open source internet search tool, I identified the IP address as being assigned to Comcast Cable Communications. After serving Comcast Cable Communications with legal process, they returned subscriber information indicated that IP address was assigned to Retro Automotive Products, 247J Sullivan Street, Claremont, New Hampshire at the time/date of the TextNow account creation. Therefore,

it can be determined that the person(s) who created the TextNow accounts associated with the two phone numbers used to send threatening/harassing text messages to Cawvey Jr. on March 25 and March 26, 2020, was using an IP address assigned with RAP's Internet connection<sup>13</sup>.

### **PINGER SUBPOENA RESPONSE**

32. (508) 738-2600 was used to send threatening/harassing text message(s) to Cawvey Jr's personal phone on March 16, 2020 (the date these text messages first began) and (413) 842-6989, (508) 927-1691, and 802-585-2824 were all used to send threatening/harassing text messages to Cawvey Jr's person phone on March 25, 2020. Using a similar process as described above, I identified the wireless provider of these four numbers as Pinger, Inc. Pinger, Inc. was served with legal process and later provided subscriber information including the account "name," the account creation date/time and the IP address used at account creation. Upon review of this information, I found the following:

- a. For the number ending in 2600: the account name was "Brad."<sup>14</sup> The account was created on February 17, 2020 from IP address 174.242.74.31 using an Apple device. The IP address was assigned to Verizon Wireless as a mobile Internet service provider. The number remained assigned by Pinger from March 16, 2020 through April 15, 2020.

---

<sup>13</sup> On July 30, 2020, I interviewed Alldredge and learned that LEFEBVRE was at work on Wednesday March 25 and Thursday March 26, 2020. I also know, based upon interviews with Cawvey Jr, that RAP has a wireless Internet connection at the business.

<sup>14</sup> LEFEBVRE's first name is Bradley.

- b. The numbers ending in 6989, 1691, and 2824 were associated with three different Pinger accounts created on March 25, 2020, from IP address 73.68.213.55, the same Comcast Cable Communications IP address assigned to RAP as described above. Two of the accounts were created using an Apple device; the third was created using an Android device.

### **APP AND SERVICE EXPLANATIONS**

33. *Grindr*: According to an open source Internet search, Grindr is a location-based social networking and online dating application for gay, bi, trans, and queer people. It is available on iOS and Android devices. The app allows members to create a personal profile and use their GPS position to place them on a cascade, where they can browse other profiles sorted by distance and be viewed by nearby and faraway members depending on one's filter settings. Selecting a profile photo in the grid view will display that member's full profile and photos, as well as the option to chat, send a "tap," send pictures, video call, and share one's precise location.

34. *TextNow*: According to TextNow's Law Enforcement User Guide, TextNow is a voice over Internet Protocol ("VoIP") service that allows its users to text and call any number in Canada and the United States. They provide users with a real phone number which can be used on any smartphone, tablet, or desktop computer or smartphone with an Internet connection. The application can be used on multiple devices under the same login at the same time. The TextNow app is available for download in iOS, Android, Windows, and Mac based systems. When a user registers for TextNow they are assigned a 10-digit phone number identifier (three-digit area code

and a seven-digit number). Upon registration, the user will enter their desired area code; if a number with their desired area code is available, the user will be assigned that number. If TextNow does not have a phone number with the user's desired area code available, the user will be prompted to enter a new area code. TextNow collects and retains basic subscriber data such as username, phone number, name (if available), email address, date of birth (if available), phone ownership from date, phone ownership to date, and registration IP address with date (if available). TextNow cautions that subscriber data is provided by the user and not independently verified by TextNow.

35. *Pinger*: Pinger, Inc. is an application developer located in San Jose, California. Pinger develops and publishes cross-platform communication applications designed to run on desktops, Android, iOS, and Windows phone devices. Depending on the application and the platform on which it is used, several of Pinger's applications allow for messaging, calling services, and call management tools. Communications are made using Wi-Fi or the user's wireless communication services. Pinger can collect and store the following information: (1) basic subscriber information including Pinger assigned phone number, a registered phone number, name, username, third-party email address, internal Pinger account ID, and electronic serial number (ESN), such as Mobile Equipment Identifier (MEID)/International Mobile Equipment Identity (IMEI), of the device, (2) transactional records including call detail records, detailed message logs, and connection records, such as Internet Protocol (IP) address information, and (3) Content of messages which Pinger retains for about 72 hours.

36. *Bandwidth*: According to their website's legal guide, Bandwidth is a nationwide communications and VoIP service provider primarily serving business customers. Many of their

customers use their VoIP services in a wholesale manner, offering services of their own together with a Bandwidth telephone number to their end users. In these cases, Bandwidth does not have a relationship to the end user or any information about the end user and how the number is being used by the end user.

### **TECHNICAL TERMS**

37. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. *Wireless telephone*: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global



positioning system (“GPS”) technology for determining the location of the devices.

- b. *GPS*: A GPS navigation device uses the Global Positioning System (generally abbreviated “GPS”) to display its current location. It often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer or smartphone connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- c. *Digital camera*: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or smartphone or by connecting the removable storage medium to a separate

reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- d. *IP Address*: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computer or smartphones on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer or smartphone attached to the Internet computer or smartphone must be assigned an IP address so that Internet traffic sent from and directed to that computer or smartphone may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computer or smartphones have static—that is, long-term—IP addresses, while other computer or smartphones have dynamic—that is, frequently changed—IP addresses.
- e. *Internet*: The Internet is a global network of computer or smartphones and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- f. *SIM card*: A subscriber identity module (“SIM”) is an integrated circuit that is intended to securely store the international mobile subscriber identity number

(IMSI) and its related key, which are used to identify and authenticate subscribers on mobile telephone devices.

- g. *Storage medium*: A storage medium is any physical object upon which computer or smartphone data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.
- h. *Trail camera*: According to an open source Internet search, a trail camera, also known as a remote camera, or game camera, is a camera placed by a photographer in areas where the photographer generally cannot be at the camera to snap the shutter. This includes areas with limited access, tight spaces where a person is not allowed, or just another angle so that the photographer can simultaneously take pictures of the same moment from different locations. Remote cameras can be placed in suspended positions, usually mounted with clamps and arms. A game camera (or trail camera) is a rugged and weatherproof camera designed for extended and unsupervised use outdoors. The images they produce, taken automatically when motion is sensed, are used for game surveillance by hunters.
- i. *Secure Digital Card*: According to an open source Internet search, a Secure Digital, officially abbreviated as “SD” is a non-volatile memory card format for use in portable devices.

- j. *Prepaid mobile phone*: According to an open source Internet search, a prepaid mobile phone, commonly referred to as a pay-as-you-go, or prepay is a mobile device such as a phone for which credit is purchased in advance of the service use. As calls and texts are made, and as data is used, deductions are made against the prepaid balance amount until no funds remain (at which time services stop functioning). A user may avoid interruptions in service by making payments to increase the remaining balance. Payment options include retail store purchases using a “refill” card stamped with a unique code (often under a scratch off panel) which must be entered into the phone in order to add the credit onto the balance, among other methods. Prepaid mobile phones and their “refill” cards can be purchased using cash at most major retails in the US. Because there is no registration requirement for prepaid mobile phones, users remain mostly anonymous.

### **COMPUTER ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

38. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer or smartphone’s hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

39. *Probable cause.* I submit that if a computer or smartphone or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or smartphone or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer or smartphone files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer or smartphone, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer or smartphone’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer or smartphone storage media—in particular, computer or smartphones’ internal hard drives—contain electronic evidence of how a computer or smartphone has been

used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer or smartphone users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

40. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer or smartphone files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers or smartphones were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs

store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer or smartphone was in use. Computer or smartphone file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer or smartphone and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or smartphone or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or smartphone or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus,

spyware, and malware detection programs may indicate whether the computer or smartphone was remotely accessed, thus inculping or exculpating the computer or smartphone owner. Further, computer or smartphone and storage media activity can indicate how and when the computer or smartphone or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer or smartphone accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or smartphone or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or smartphone or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer or smartphone may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic



and timeline information described herein may either inculcate or exculpate the computer or smartphone user. Last, information stored within a computer or smartphone may provide relevant insight into the computer or smartphone user's state of mind as it relates to the offense under investigation. For example, information within the computer or smartphone may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or smartphone or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer or smartphone works can, after examining this forensic evidence in its proper context, draw conclusions about how computer or smartphones were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer or smartphone evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer or smartphone is evidence may depend on other information stored on the

computer or smartphone and the application of knowledge about how a computer or smartphone behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer or smartphone was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

41. I know that when an individual uses a computer or smartphone to download and use third-party apps for the purpose of stalking and/or harassing someone, the individual's computer or smartphone will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer or smartphone is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer or smartphone is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer or smartphone used to commit a crime of this type may contain: data that is evidence of how the computer or smartphone was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

42. *Necessity of seizing or copying entire computer or smartphones or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer or smartphone's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer or smartphone has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. *Technical requirements.* Computer or smartphones can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer or smartphone hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. *Variety of forms of electronic media.* Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

43. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer or smartphone-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

44. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or smartphones or storage media, the warrant applied for would permit the seizure and review of those items as well.

**CONCLUSION**

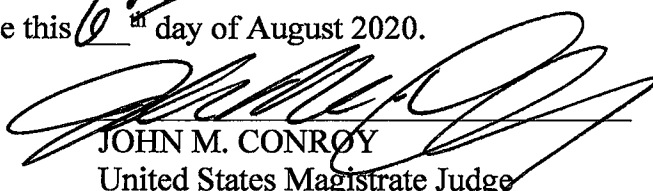
44. Based on the foregoing, I submit probable cause exists to search the residence, more specifically described in Attachment A, for the evidence delineated in Attachment B.

Dated at Burlington, in the District of Vermont, this 6<sup>th</sup> day of August 2020.



Jeffrey W. Stephenson  
Task Force Officer  
Federal Bureau of Investigation

Sworn to and subscribed before me this 6<sup>th</sup> day of August 2020.



JOHN M. CONROY  
United States Magistrate Judge